DSTO

Secure Real Time Group-Oriented Communications

M.K.F. Lai

DEPARTMENT ◆ OF DEFENCE

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Secure Real Time Group-Oriented Communications

M.K.F. Lai

Information Technology Division
Electronics and Surveillance Research Laboratory

DSTO-RR-0055

ABSTRACT

This paper is part of the document series produced under the HQADF sponsored task 'D6: A Security Architecture for Large, Distributed Multimedia Systems'. The first of two main aims of this paper is to identify an internationally standardised real-time multi-media multi-point communications platform, on which mission-centric group-oriented applications may be developed using commercially available products. The second aim is to investigate the protocol security requirements to support the identified platform. This paper specifically focuses on the trustworthiness of a platform-enabling mechanism known as GCC (Generic Conference Control) Provider. A potential outcome could imply the possibility of "BLACK Conferencing", where only encrypted conference information is processed by conference bridges or multi-point control units.

APPROVED FOR PUBLIC RELEASE

DEPARTMENT OF DEFENCE

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Published by

DSTO Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury, South Australia, 5108

Telephone: (08) 259 7053
Fax:(08) 259 5619

AR No. 009-398
September 1995

APPROVED FOR PUBLIC RELEASE

Secure Real Time Group-Oriented Communications

Executive Summary

Information dominance at the tactical, operational and strategic levels of the armed forces will be the pre-eminent force multiplier in current and future battlefields. The Australian Defence Force (ADF) has a stake in the outcome of mastering Command, Control, and Communications (C3) technologies. Any successful prosecution of military operation depends on their effectiveness [1].

This paper focuses on the emerging communications technologies that are specifically group-oriented. These technologies, known as real-time multi-media multi-point communications, mimic the physical meeting environment for multiple parties at geographically dispersed locations. They enable group-oriented discussions and decision processes required by commanders.

The first of two main aims of this paper is to identify an internationally standardised real-time multi-media multi-point communications platform, on which mission-centric group-oriented applications may be developed using commercially available products. A communications platform is a system that supports its client applications to communicate. What makes a platform standardised are the protocols that specify the interactions between the platform components and client applications. The relevant protocol standards are called the T.120 series of recommendations [26] developed by the International Telecommunication Union.

The second aim is to investigate the protocol security requirements to support the identified platform, based on the DSTO proposed contemporary military information security philosophy [2]. The goal is to indicate a direction towards the paradigm for "BLACK Conferencing", where only encrypted conference information is processed by conference bridges or multi-point control units. This paper specifically focuses on the trustworthiness of a platform-enabling mechanism known as GCC (Generic Conference Control) Provider because of its security-relevant actions and conference service supports. To allow greater flexibility with respect to security architecture support, there are two concerns in the T.124 recommendation [29] of GCC specification where it is believed that Defence may voice its requirements.

This is a blank page.

Author

Lai M.K.F.
Information Technology Division

Dr. Lai received his B.Sc. (Mathematical Science) First Class Honours degree in 1984, followed by his Ph.D. in Combinatorial Group Theory completed in 1987, both from the University of London. He is currently the Senior Research Scientist in the Information Security Section of Trusted Computer Systems Group at DSTO. His interest coincides with that of his employer.

This is a blank page.

Contents

This is a blank page.

1 Introduction

Information dominance at the tactical, operational and strategic levels of the armed forces will be the pre-eminent force multiplier in current and future battlefields. The Australian Defence Force (ADF) has a stake in the outcome of mastering Command, Control, and Communications (C3) technologies. Any successful prosecution of military operation depends on their effectiveness [1].

In assisting commanders to conduct their functions and to achieve their mission, current C3 technologies have been relatively more successful in those areas that are heavily based on doctrinal procedures. There are, however, other areas that have tended to be neglected. Specifically, areas involving group consensus, such as multi-party conferencing, have not been focused on until recently. After the Desert Storm experience, local and allied military strategists have started to appreciate the increasing requirements for command and control support at the operational as well as strategic levels, particularly for joint or combined missions involving national services or multi-national forces. In contract to the tactical level environment, doctrinal procedures play a smaller part at these levels. Most operational or strategic military functions are conducted via group-oriented discussions and decision processes among commanders and their subordinates.

This paper focuses on the emerging communications technologies that are specifically group-oriented. These technologies, known as real-time multi-media multi-point communications, mimic the physical meeting environment for multiple parties at geographically dispersed locations. They enable group-oriented discussions and decision processes required by commanders. The first of two main aims of this paper is to identify an internationally standardised real-time multi-media multi-point communications platform, on which mission-centric group-oriented applications may be developed using commercially available products. A communications platform is a system that supports its client applications to communicate. What makes a platform standardised are the protocols that specify the interactions between the platform components and client applications. The second aim is to investigate the protocol security requirements to support the identified platform, based on the DSTO proposed contemporary military information security philosophy [2]. Currently, the high cost of high grade security as a percentage of total project costs presents a significant concern in Defence procurement[1]. Success of the standard-based platform would allow military users to choose commercial group-oriented products predominantly based on mission-suitability.

The paper is organised as follows. In Section 2, the role of military group-oriented command and control (C2) and their near and far term development plans are examined. Following the proposed contemporary military philosophy, Section 3 discusses the requirement for an internationally-standardised real-time multi-media multi-point communications platform, on which mission-centric group-oriented applications including multi-media conferencing are developed. The existing secure audio conferencing facility with Defence is revisited in Section 4. It is used to highlight the new functionality and enhancement that must be achieved in the identified multi-point communications platform. An "ideal" configuration for secure multi-media conferencing is presented in Section 5. Finally, the necessary secure architectural support and enabling trusted architectural components are discussed in Section 6.

1. This situation was revealed during discussions at Defence Security Workshop, sponsored by the HQADF, Canberra, between 1-2 June of 1994.

This is a blank page.

2 *Group-oriented Communications in the Military Context*

A typical use of group-oriented communications is the inter-headquarters real-time multi-point audio-video conferencing facility. Operational-centric subjects, tables, maps, and target imagery can be exchanged or simultaneously displayed among authorised group participants while engaging in warfare analysis or strategic planning discussions. Such virtual conferencing could be equipped with the aids of digitally exchanging control measures using electronic pens and with the observations of unit positions on a common digital display.

Occasionally, subordinates from the battlefield can be brought into a virtual conference to brief on the latest tactical situations. This is seen as a productive and cost-effective replacement for the commanders' needs to consume valuable time in having subordinate commanders report individually over voice-only transmission links or at some coordinated contact points. However, this virtual conference would have to be achieved over a number of mobile, deployed and fixed networks and possibly with less capable equipment, operating over some disadvantaged links for some tactical zone users. At the other end of the command chain, using the same technology, a higher echelon of the military command or the national government authority can be invited to receive conference outcomes while the conference is being concluded. More military-specific application scenarios are presented in [5].

At the enterprise level in the Department of Defence, group-oriented communications technology enables strategic multi-site, multi-agency decision support. The nature of both military and civilian activities shifts from independent manual processes to using networked information systems in support of operational objectives. Batch quality executive summaries with audio-visual commentary from multiple sites can be accessed via on line querying. Various mission-driven tasks can be brought under a pivotal control through the group-oriented technologies, such as those developed around the idea of computer-supported cooperative work (CSCW). These scenarios are found to be applicable to all mission levels because of their high compatibility with the human nature of group consensus seeking.

2.1 Near and Far Term Development Plans

Military strategists are beginning to explore the use of group-oriented technologies for strengthening the C3 military functions. This trend has been shown both locally [6] and [7], and from overseas [8]. Investigations on specific group-oriented applications are beginning to gather momentum. Both [9] and [10] concern video conferencing, which is seen as a basic group-oriented application. The recent military communications conference, MILCOM 94 at Fort Monmouth, has also registered a number of development initiatives for video conferencing at the operational level [11], [12], [13] and [14]. These efforts focus on the near term plans based on traditional technologies. They basically are developing the video conferencing application as a stand-alone system. Encryption is used "indiscriminately" on all communication links in order to protect the whole system. This implies inefficient use of the global network and inflexible communication application functionality.

The fundamental focus in information technology is shifting from storage-oriented computing to communications processing and from the added value of the central processing unit to the added value of the "network". The future "network" could be viewed as the computer of today [15]. The performance measure of the new era will be "billions of bits per second" rather than "millions of instructions per second" as noted by Mundie of Microsoft. The emerging multi-point communications technologies will encompass more than just video conferencing. A user will have his/her own option to choose a communicating media best suited to his/her current activity, regardless which communication modes his/her many

communicating partners may use. There also will be computer-supported cooperative work (CSCW), multi-site battlefield and training exercise simulation, and others. All of these require diverse network or computing resources, wherever available, on an "on-demand" basis. To initiate far term planning, it is essential to identify a generic real-time multi-point multi-media communications platform based on the emerging technologies and associated standards. The identified platform should be able to present a virtual group-work environment, such as group address scheme, conductorship, conference proceeding control, and others, upon which mission-specific applications can be built.

In the next section, a DSTO proposed contemporary military philosophy is followed in the investigation of real-time group-oriented C3. This philosophy has been demonstrated through DSTO's Stubs Development [16] and DORIC Program [6]. The section will discuss the rationale for a group-oriented communications framework and the necessary technologies to implement the chosen generic real-time multi-point multi-media communications platform.

3 *Military Communications Technology Efforts*

Military communications technology efforts have to be related closely to Defence programs that focus on either modernising existing capabilities through upgrades, or designing replacement advanced systems to meet new information needs.

3.1 Increasingly Capable Defence Messaging System

The proposed Defence messaging capability extension from ACP 127 to ACP 123[2] conformance systems is an example of modernisation through upgrading. Incremental security enhancements through the use of Message Security Protocol (MSP)[3] and the placements of cost-effective retrofit compact trusted security peripheral devices to provide the goal writer-to-readers security for Defence store and forward text-based messaging service users are being developed [7]. Such developments represent one of the major near-to-middle term communications capabilities for Defence [4] and [17].

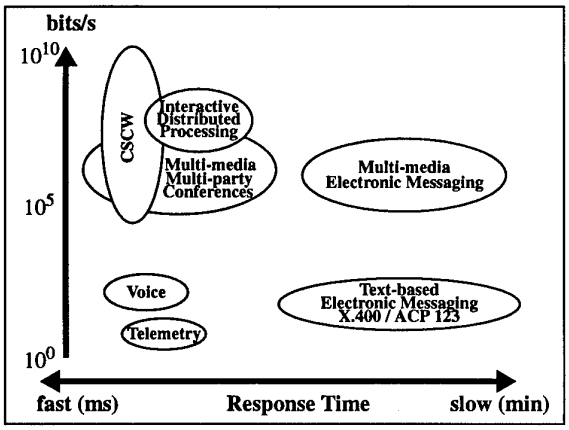

Figure 1 The Bandwidth and Timing Nature of Some Group-oriented Applications

The Defence messaging system will serve a wide spectrum of military communications scenarios. This spectrum is represented by the left half of the diagram in Figure 1. The messaging system provides appropriate methods for encapsulating different information types (such as audio, video, graphics) within the message body part structure. In using this system, the timing between the sender's action and the recipients' reactions is not expected

2. Allied Communications Publication (ACP) 123 is an international collaborative military effort based on international electronic messaging standards ITU-T X.400 series.

3. MSP belongs to the US SDNS (Secure Data Network System) suite of protocols, which are designed to address information system security. It focuses on electronic message security. Its function is to provide the method to exchange security-related information between message writer and readers. MSP currently is being adopted by Australian Defence, subject to its further development to meet the Australian national requirements, and to international approval to become an annex of ACP 123. The Australian proposal of an additional national field into the MSP header was initiated by the D6 team of DSTO and submitted through HQADF and the national security authority. The result will be reflected in the re-issue of the MSP Specification in the first half of 1995. Currently, the D6 team is actively designing the mechanisms belonging to the national field which are specific to Australian Defence requirements.

to be critical. Hence, the messaging system supports only non real-time communications. The right half of the diagram (Figure 1) captures (old and new) real-time secure communications applications. These new applications will require protection using some carefully designed advanced security devices in order to achieve their full potential in the military context. These devices could form the foundation for building the far term Defence communications capabilities.

3.2 Designing New Generation Real-Time Multi-point Communications

Currently, voice (in the form of one-to-one dial-up telephone calls or all-informed combat net radios) is the only relatively mature secure real-time application available to the military. Many others remain to be realised, even for civilian use, and are among the most active research and development areas. Current technologies are able to address only two real-time communications scenarios, namely one-to-one and broadcast. Other secure scenarios, such as one-to-selective-many or selective many-to-many, have not been addressed sufficiently. For example, a current technology secure audio conference facility with a selectable participant list is comparatively less flexible and it requires Defence controlled RED conference bridges[4].

Although the internationally approved messaging standards (such as X.400 and ACP 123) have provided a common framework for handling multi-media store and forward communications, there is not an established and universally agreed common framework for conducting real-time group-oriented applications involving different information types. Experimental prototypes are being developed and tested on an application by application basis. These prototype applications include shared electronic white board, computer-supported cooperative work (CSCW), video conferencing, and video broadcast [18], [19], [20], [21], [22] and [23]. Each of them is tapping into the network resources directly through its individual application-specific interface, rather than through some standardised interfaces designed for generic group-oriented applications. Such current efforts largely focus on the network efficiency for transporting the different information types or on the performance of various media type coding schemes, instead of co-ordinating group work environments suitable for multiple simultaneous participants. Very little has been done on how various group-oriented applications should complement each other or be combined together at the user level to form a unified business or operational tool [24].

3.2.1 The Rationale for a Secure Multi-point Communications Platform

Developing individual security protection separately for each application over open networks would not only increase the purchasing cost, but also limit the scope for using commercial off the shelf (COTS) products and hence prolong the acquisition time in bringing new applications to military users. Moreover, the Defence Organisation does not always have sufficient resources to investigate how security should be provided to every potential group-oriented application for military use.

A better approach, guided by the philosophy in [2], would be to concentrate on the security provision of a common generic real-time multi-point group-oriented communications platform, similar to the current efforts on the security of the ACP 123/X.400 based messaging platform. In most real-time group-oriented applications, human participants are present at each end-point to conduct their communications instantaneously - for example, traditional telephone users. The aim is to derive a multi-point communications platform architecture that

4. A RED conference bridge is a conference bridge which may process sensitive information or data. Generally, an information transferring network element is called RED if it handles classified information in the clear. The current setting for secure RED audio conference will be discussed in Section 4.

does not require sensitive (RED) group communication related information or data to be processed by intermediate nodes of the traffic-carrying networks. By providing security protection based on the platform, the platform effectively becomes a security barrier that protects the communicating end-users' information. For example, a BLACK conference bridge, which provides a conference bridge facility that is not required to handle the clear content of audio or video conference traffic streams, is a major goal for the architecture development.

3.2.2 The Role of the Human Participant

The assumption of human presence at each communication end-point is significant when a security architecture for communications over open networks is considered. This assumption forms the basis of manual review and confirmation of security critical actions by a communicating end-user before some specific information or data actually is delivered to the connected open network for transportation. In this scenario, a trusted path must exist for logically connecting the human user and his/her confirmable actions undertaken by trusted security components embedded within the architecture. The main security aim is to design an "easy to verify" and "easy to implement" trusted path within a common real-time multi-point communications enabling platform that supports *all* group-oriented applications. In such an architectural arrangement, the explicit trusted path implementation *within* an application would become superfluous.

3.2.3 Essential Platform Characteristics

A secure platform should not impose any special security requirements on the applications (such as video conferencing, shared white board and CSCW) that it supports. The net result broadens the scope to use commercially available products and therefore reduces the acquisition cost. Defence project managers can focus on acquiring applications that best meet users' functional requirements. Moreover, if the revelation of RED information does not occur in transit, the opportunity to use publicly available open network resources is widened. Finally, a common multi-point communications platform implies improved interoperability. The platform should include the necessary protocols for end terminals and group-oriented network elements to exchange information on their communications capabilities. The end terminal-specific information includes the types of audio/video coding and decoding (codec) schemes available, the provision of security, and so on. On the other hand, network elements can exchange information concerning the types of group-oriented services (such as conference conductorship support, and the ability to support parallel conferences and the ability to provide conference profiles).

3.3 A Framework Based on the T.120 Series of Recommendations

The international standards body Telecommunication Standardisation Sector of International Telecommunication Union (ITU, formerly CCITT) focuses on a growing number of services having as their common characteristic the transmission of speech together with other information reaching the eventual users in visual form. According to their recommendation H.200 [25], such services conveniently have been referred as "audio-visual services". The organisation further recognises that this set of services should be treated in a harmonised way. While these services may be distinguished easily in terms of their user-application, the standardisation process still can seek the greatest possible harmonisation with respect to their common features of speech, moving, or still picture signal transportation, associated controls/ indications, and also telematic auxiliary facilities.

Three main classes of standards, namely "service definition", "infrastructure", and "systems and terminal equipment", have been defined in H.200 for providing harmonisation of the audiovisual services. Among the three, the "infrastructure" class is the most important as it

defines the communications signals which flow on unrestricted digital bearers of established network connections. This class encompasses network configuration, frame structures, control/indications, communication/intercommunication, and audio/video coding. In particular, it includes a standard framework, consisting of the ITU-T T.120 series of recommendations, for real-time multi-point communications.

In this paper, the above series of recommendations is considered as a possible candidate framework on which third party general purpose or military mission-specific group-oriented applications may be built. The series is presently being developed by the ITU, through its subgroup SG 8. Member technical contributions are generated from a wide cross section of the high technology industry including semi-conductor manufacturers, computer hardware vendors, software developers, telecommunications services, network hardware and software suppliers, and systems integrators. Currently included in the series, there are eight draft recommendations T.120 [26], T.122 [27], T.123 [28], T.124 [29], T.125 [30], T.AVC [31], T.126 [32], and T.127 [33], each possessing varying degrees of maturity.

3.3.1 An Overview of the T.120 Series of Recommendations

These recommendations (especially T.122 and T.125) are intended to provide a multi-point data service that has applications in all forms of multi-media communications. They define the support for the establishment of a conference (or a group) of network elements (such as conference terminals). Within the context of these recommendations, a conference is described as a group of geographically dispersed nodes that are joined together and that are capable of exchange of audio-graphic and audio-visual information across various communications networks.

Participants taking part in a conference need not have identical media handling capabilities. The various types of capabilities include audio-only (telephony), audio and data (audio-graphic), audio and video (audio-video) and audio, video and data (multi-media). They will be discussed in more detail in the latter sections. Mechanisms, in the form of protocol elements, are specified in these recommendations for identification of the participating elements and for conference specific capability and information exchange. From the security view point, the interest in the T.120 series is mainly due to the provision of these standardised mechanisms. In Section 6, there will be a discussion on the interfaces between these mechanisms and military grade security peripheral devices for peer authentication and confidential group communication establishment functions.

3.3.1.1 Multi-point Control Units and Independency of Network Types

A typical conferencing topology is shown in Figure 2. Extra equipment is required in the form of one or more multi-point control units (MCUs), also generally known as conference bridges. A MCU typically is located at the hub of a star or sub-star topology. It provides the duplication and switching of a participant's data traffic streams to other authorised participants. The star topology is preferred over others, such as a mesh topology, mainly because of its reduction in the required number of network connections relative to other topologies.

The T.125 Multi-point Communications Service (MCS) [30] and T.124 Generic Conference Control (GCC) [29] are combined to enable a terminal to participate in multiple conferences if authorised to do so. Within the military context, this implies that these simultaneous conferences may need to be conducted at different classification levels (for example, one is at the Secret level while another is at the Top Secret level). It follows that cryptographic separation of individually classified conferences may be an appropriate option for ensuring that both the integrity and confidentiality of the communicating information within a conference are maintained.

If a MCU is not required to handle or process any sensitive RED information, the system trust of the MCU and its associated T.120 protocol implementations becomes less critical. The function of the MCU is therefore de-coupled from the provision and maintenance of communicating information integrity and confidentiality. It also follows that the availability of the conference service is not diminished because any T.120 conformed MCU should theoretically provide a similar service. It therefore would not be necessary to specifically design MCUs that meet Defence security requirements.

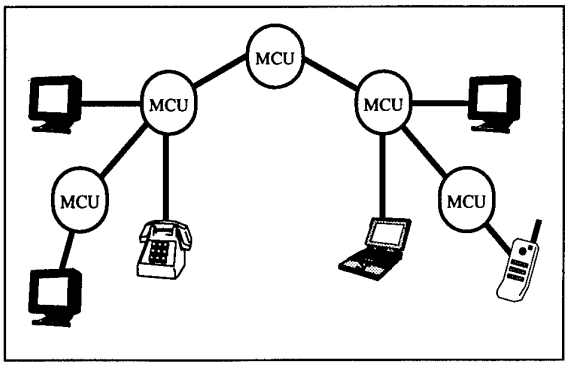

Figure 2 Multi-media Conferences Using MCUs

No conceptual constraint is placed on the volume of information transmitted within the various media types. The T.120 protocols have the capability to organise appropriate capacity and priority for conference traffic streams, within the constraints imposed by the type of network and connections established thereof. All network types: PSTN[5], ISDN[6], CSDN[7], PSDN[8], ATM B-ISDN[9], and wired or wireless LAN[10] should be able to carry T.120 protocol data and they therefore implicitly provide the capability for seamless interworking of applications on terminals connected to different networks.

3.3.1.2 Conference Controls and Conversation Information Management

Conference controls are provided by the T.124 protocols. Through these protocols, the conference convener or conductor may control the conference participation and the information that flows in that conference. If cryptographic separation is enforced within the conference, the convener or conductor must be able to safely invoke an associated key management system to assign and distribute a new session key whenever he wishes to invite new conferees or to lock out existing conferees. Conversation speech and video signals are transmitted on channels that are separate from that carrying the core T.120 protocol data such as MCS and GCC protocol data units. There therefore must be a separate provision for the real-time control of these signal channels. Such provision is achieved by the recommendation T.AVC Audio Visual Control (AVC) [31].

In Sections 5 and 6 below, it will be shown how the T.120 based multi-point communications framework can furnish the foundation for strengthening the security protection for group-

5. Public Switched Telephone Network.
6. Integrated Services Digital Network.
7. Circuit Switched Digital Network.
8. Packet Switched Digital Network.
9. Asynchronous Transfer Mode Broadband Integrated Services Digital Network.
10. Local Area Network.

oriented applications. Moreover, there will be a discussion on the security deficiencies currently existing within the latest draft recommendations, that may require appropriate remedies in order to meet military requirements.

3.3.2 The Industrial View of the T.120 Protocols

There are a number of industrial fora/consortia/alliances that are focusing on multi-point multi-media communications. Among them, the Personal Conferencing Work Group (PCWG), led by Intel, seems to receive significant media attention, following its release of the Personal Conference Specification (PCS)[11] to its member companies. Current PCWG membership exceeds 100 companies and includes AT&T, Lotus, Hewlett-Packard and DEC.

Having committed more than US$100 million to their conferencing technology [34], it appears that Intel's objective is to promote the use of video conferencing related modules (such as the software-only Indeo codecs, hardware and software based MPEG decoders and graphics accelerators) from the desktop. Time-consuming tasks for retrieving software instructions and data from memory are needed to drive these modules. They seem to believe that the demand for greater central processing unit (CPU) resources arise because of the frequent and rapid executions of these tasks.

There is however another school of thought. It emerges from the bandwidth-driven world and is also gaining many supporters [15]. The leader of this school is MicroUnity, which is financed by both Tele-Communications Inc. and Mircosoft. MicroUnity's goal is a software programmable general-purpose media-processor that can run at above 400 billion bits/s and could receive decompression codes and other protocols, algorithms and services over the network, with the video to be displayed in real-time. This media-processor may leave the CPUs to serve as a minor peripheral to manage only documents on the screen, pop up needed information from database holdings, perform simulation or visualisation, and otherwise enrich multi-media conferences.

Between Intel's and MicroUnity's visions, the question that remains to be answered is whether CPUs will subsume media-processors, or whether media-processors will make the CPU functions redundant in the age of advancing ATM technology[12]. Finally, there is IBM, which is pushing its own multi-media group work architecture, called Lakes Collaborative Networking Architecture. The company is claiming support from industry.

While each of these industrial alliances is claiming that its specification or development can either support or accommodate T.120 protocols, they clash repeatedly in open forums over the merit of their competing proposals [35] and [36]. This consequently means extra confusion for corporate users, such as Defence, when choosing the appropriate systems or products. It is hard to keep an accurate list of which vendors support which specification because it is common for vendors from opposing consortia to have company members sitting on each other's committees. Nevertheless, the T.120 series of recommendations remain the only common technology in the area of multi-point multi-media communications. It is seen as the only available mechanism that may be able to guarantee the much needed interoperability for emerging group-oriented applications and their interworking. A number of multi-national companies recently have announced their support of T.120-based technologies [37], [38]. Locally, Telstra began their Multi-media Conferencing Trial Program in May 1995 [39]. One of the goals is to free customers from the requirements to

11. Public release is not expected soon.
12. The ATM technology is eclipsing the difference between an internal hard drive memory and an external networked data storage. An ATM LAN or even WAN could function as a motherboard backplane, indicated by the statement "the future network is today's computer" in [15].

purchase their own multi-point control units or conference bridges, which currently are the most expensive components in the provision of corporate video conferencing facilities. The Trusted Computer Systems (TCS) Group at DSTO is pursuing a similar direction of using the T.120-based technologies. The aim is to achieve the "BLACK multi-point control unit functionality" for classified multi-point communications. This concept will be explained in detail in Sections 5 and 6 below.

3.3.2.1 Where Defence Should Apply its Influence

Many parts of the T.120 series remain incomplete. Resolutions for some draft recommendations are not due until later this year. Defence can play a part, possibly through collaborations with allies to ensure a critical mass. Influencing the final T.120 recommendations into meeting the military requirements would prove to be advantageous to Defence. From the Government and particularly the Defence perspective, it may not be appropriate to become involved with an industrial alliance directly. However, Defence is an active member of ITU and so are the allied military organisations and leading companies of the aforementioned alliances.

Locally through its Science and Technology Program DSTO, Defence retains healthy relationships with the two national telecommunications suppliers Telstra and Optus Communications, based on respective Memorandums of Understanding (MOUs). Both companies are influential players in the standards fora and they have assisted Defence to sway the international communications standardisation in the recent past [6].

This is a blank page.

4 The Existing RED Conference Facility within Defence

This section presents an overview of the currently available secure conference facility and indicates where new functionality and enhancements may be achieved with emerging technology based on the T.120 series of recommendations.

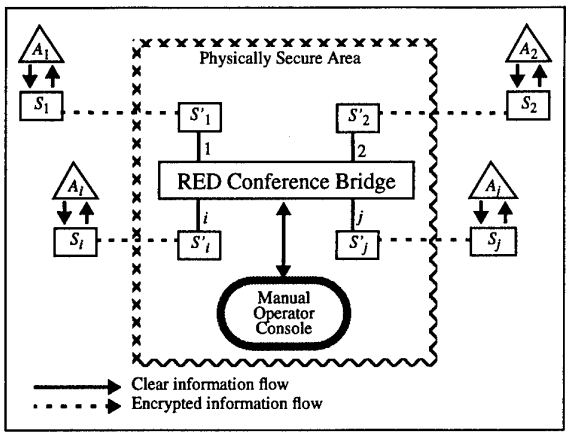

Figure 3 The Current Configuration for Secure Audio Conferencing

Defence presently has a secure audio conferencing facility for mutually exchanging national security classified information. This facility is based on the security services enabled by Speakeasy communication terminals. Its functionality is achieved by the provision of a RED conference bridge in a physically secured enclave [40]. Following from the recommended conferencing configuration, which is summarised in Figure 3, each conferee A_i is connected to the conference bridge via a connection secured by a pair of Speakeasy terminals (S_i, S'_i). The conference is arranged by a local manual operator who also establishes the secure working on the pair of Speakeasy terminals on each assigned connection i of the conference bridge, in conjunction with the corresponding conferee A_i. At the conference bridge, there is an audio mixer. It sums the audio signals received from all the assigned connections in the conference. The audio signal from connection i subsequently is subtracted from a duplicate of the sum before the resultant is sent to the transcoder of connection i.

4.1 Congenital Inflexibility

With this configuration, a conferee cannot obtain direct peer-identity authentication of the others and must rely on the manual operator, who must be cleared to the highest classification level at which a conference may occur. The confidentiality and integrity of audio information cannot be achieved in the direct speaker-to-receivers mode. The RED conference bridge in the middle must handle clear information.

The deployment of a manual operator makes the conference configuration inflexible since any conference must be pre-arranged beforehand. Even at the same classification level, simultaneous (parallel) conferencing operations (such as merging conferences, dividing a conference into subconferences or momentarily locking out some participants) cannot be organised dynamically by the operator with the RED conference bridge. Separate operators with associated conference bridges are required to manage and control separate conferences.

The notion of a conference owner does not exist in this configuration. The conference convenor, who initiates a conference, has no direct control over the conference. Every conferee must rely on the manual operator to inform of another participant's joining and leaving the current conference. As there is only one communicating channel within the conference, the operator has to interrupt the conference conversation in order to properly advise the latest participant list. Finally, the current setting does not easily allow the integration of other communications capabilities such as video, electronic white board or the sharing of electronic documents.

4.2 Manual Operator Dependency

With a RED conference bridge, no trusted paths between conferees are possible unless a trusted element is available at the conference bridge facility to assure the competent handling of sensitive information. Due to its complexity, it is difficult and expensive to guarantee the conference bridge system assurance. No currently existing conference bridge can therefore be sufficiently trusted to autonomously conjugate the trusted paths between conferees. The manual operator is employed solely to provide the missing trust for conjugating the security-critical trusted paths. Activation of encryption/decryption functions within the physically secure conference bridge facility needs to be delegated to the operator. Conferees are assured by the operator that their encrypted information is decrypted correctly by corresponding Speakeasy terminals; mixed, duplicated and switched by the conference bridge; and then encrypted by the same Speakeasy terminals before being transmitted to the respective authorised conferees.

5 *Ideal Secure Multi-media Conferencing*

In order to eliminate the expensive RED secure conferencing bridge enclave, the immediate prerequisite is to free the conference bridge facility from operating the encryption/decryption functions. This in turn requires the future audio conference bridges or the more general multi-media MCUs to be BLACK. A MCU is called BLACK if it can handle, duplicate and switch encrypted conversation signal streams.

Since a BLACK MCU processes only encrypted or insensitive data, RED data mixing at the MCU of conference information is not possible. It therefore implies that the conference conversation data mixing function has to be pushed into every conferee's terminal (RED zone). This secure multi-media conference configuration based on BLACK MCUs, with no RED mixing function, is called BLACK conferencing and it is depicted in Figure 4. Moreover, BLACK conferencing allows a user to participate in more than one virtual conference via a single terminal. Subject to his/her authority, the user employs the security peripheral to control the flow of information between the conferences in which he/she participates.

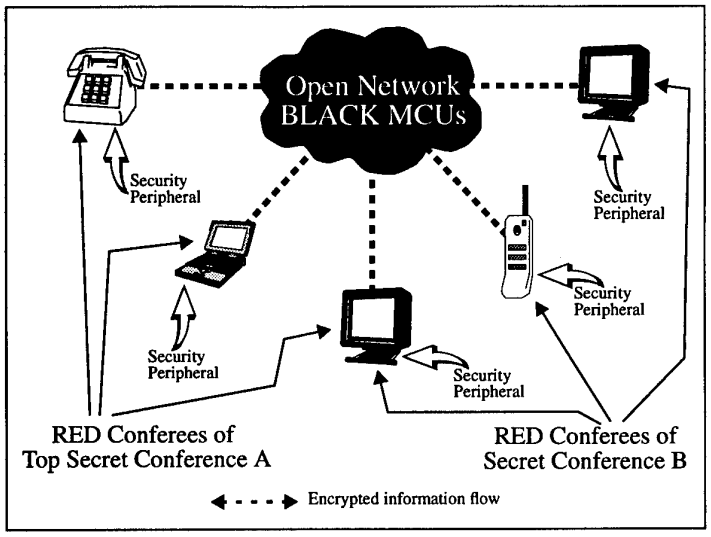

Figure 4 The Ideal Secure Multi-media BLACK Conferencing

5.1 *Security Peripheral*

In addition to control the information flow between conferences, security peripheral devices (Figure 4) are necessary to provide user authorisation, conferee mutual authentication, conference conversation information confidentiality and integrity. It also guards any unauthorised data leakage from a conferee's RED zone through the connection to the necessarily untrusted MCUs belonging possibly to some open networks. The unauthorised leakage is not a major concern in an audio only conference because a conferee's RED zone consists of only the traditional memory-free telephone. However, in a multi-media conference, a conferee's RED zone typically encompasses at least a computer or workstation belonging to a RED LAN. Without a security guard mechanism properly allocated, an attacker's Trojan Horse program easily could expose the conferee's connection to the MCUs of some open networks for the purpose of leaking sensitive information stored in the conferee's RED zone.

The net effect of these security devices on the conference configuration is that only the encrypted or authorised insensitive traffic is being carried over the point-to-point physical connections between the conferees' terminals and the MCUs. These security devices interact with the multi-point communications platform through the standardised interfaces and not with individual end systems in the RED zones. As far as protecting conferees' information is concerned, the network security specific requirements therefore have been shifted from the end systems. The result is expected to widen the choice of COTS end system selection.

5.2 *Logical-Physical Separation Characteristic of MCS*

Being the only open framework available is only one of many reasons for choosing the T.120 series of recommendations to form the framework of a future Defence multi-point communications platform. Another significant point is that the T.120 series possesses a realistic potential to enable the aforementioned BLACK conferencing or group work.

The series provides the standard layering approach to allocate the various standard mechanisms for implementing the multi-point communications platform. A layer provides the services used by the layer above. Interactions between two adjacent layers are conducted via the service access points at the layer boundary. In particular, T.125 specifies the multi-point communications service (MCS) layer protocols. This MCS layer provides the upper layers with the logical channels for carrying conferees' conversation data among subsets of conferees. A logical channel is effectively a unique address within a conference. There are different types of logical channels for carrying different types of conferees' conversation (speech, video, and others) as well as conference control information. Logical channels are mapped by the MCS onto the physical connections of the lower layers. The upper layers do not need to know these physical connections or any structural format of the traffic that they carry.

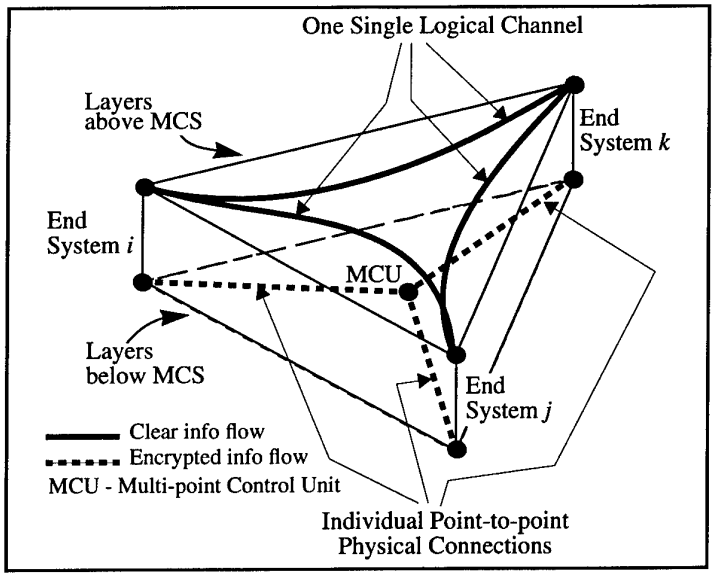

Figure 5 The Logical-Physical Separation Characteristic of the MCS Layer

In simplified terms, the MCS organises the multiplexing of the upper layer logical channels onto the physical connections. Peer MCS Providers at the conference end-points and MCUs multi-laterally recognise the logical channels, via the usage of Channel IDs that are unique within a conference. Requests for actions and responses to requests are coordinated via the

MCS protocols. Upon receiving a request from another MCS Provider, the MCS Provider at a MCU can instruct the duplication and switching of specific physical connection contents at the physical connection level according to the logical channels associated with the contents. This main MCS characteristic of logical-physical separation is summarised in Figure 5.

In the next subsection, how to make use of this characteristic to achieve the confidentiality and integrity protection for BLACK conferencing will be discussed.

5.3 Induced RED-BLACK Separation Characteristic of MCS

Typically, T.125 provides the functionality for an authorised conferee to own some logical channels that carry his conference conversation data. The owner has the ability to control which other conferees should belong to his logical channels. The usage of these logical channels is understood by all upper layers that MCS serves. Contents of some of these logical channels should be meaningful only among the intended conferees, and the channel membership need not include any MCUs. Client applications at the upper layers assume that the conversation data carried in a logical channel simultaneously will reach all the conferees belonging to the channel.

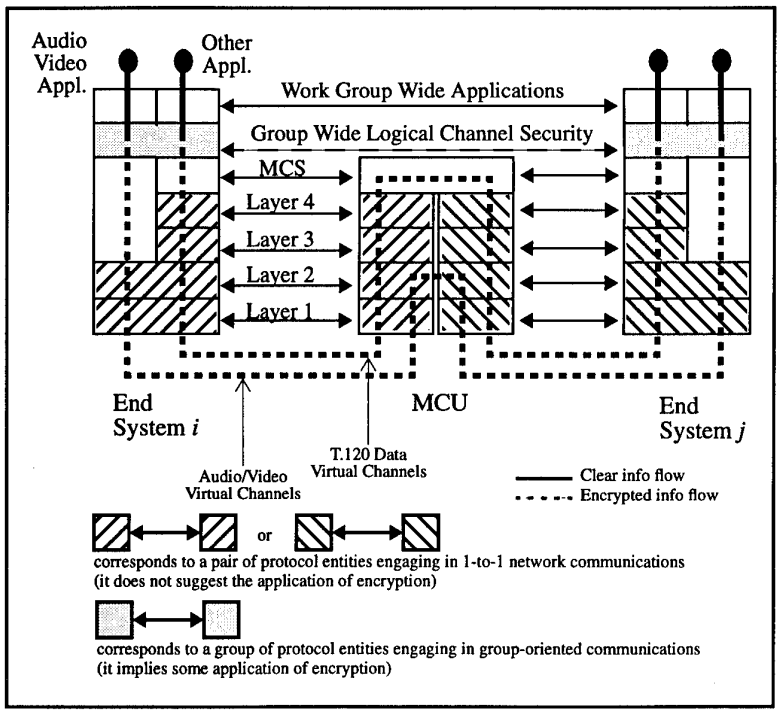

Figure 6 Some Security Function Placement within Standardised Protocol Stacks

Among MCS's upper layers, the encryption/decryption function of the security peripheral can be inserted. It may be viewed simply as just another client application. As long as the (human) owner of a logical channel can establish securely a common session channel key[13] with only the conferees whom he/she wishes to include in the channel, via a capable key management scheme, his/her conference conversation data can be encrypted. The encrypted

13. A session channel key is referred as a cryptographic key that is unique to the associated channel within the active conference session.

data then is carried, over the designated logical channel to authorised recipients who would have had the necessary session channel key to unravel the channel owner's clear conversation data (Figure 6).

It therefore follows from the MCS's logical-channels-to-physical-connections mapping function that information carried over a logical channel and over the physical connections may be viewed in two quite distinct ways. On the one hand, the contents of a logical channel, which excludes MCUs, is regarded as RED information. On the other, the traffic of the physical connections, which may include MCUs, is regarded as BLACK information. This naturally induced RED-BLACK separation characteristic of MCS has to be enforced by the security peripheral devices that collectively provide the conference (work-group) wide logical-channel-based security, as shown in Figure 6. The basic functional blocks of the standardised protocol stacks of Figure 6 are described in T.123, which focus on audio-graphical and audio-visual tele-conferencing applications.

6 *Conferencing and Group Work Support Functions*

In creating an appropriate environment for geographically distributed audio-visual or audio-video conference and group work collaboration, there are a number of functions that are essential to the effectiveness of the environment. This section will consider the security-critical aspect of these functions and examine the appropriate security enforcement.

6.1 Conference Call Set-up over Wide Area Networks

A typical conference call setup would consist of three phases, namely Phases A, B, and C of Figure 7. These three phases are explained in the following subsections. They involve establishment of peer-to-peer layer communications, which starts at the physical layer and finishes at the MCS layer. Placements of the associated communication protocols are shown in Figure 7 also.

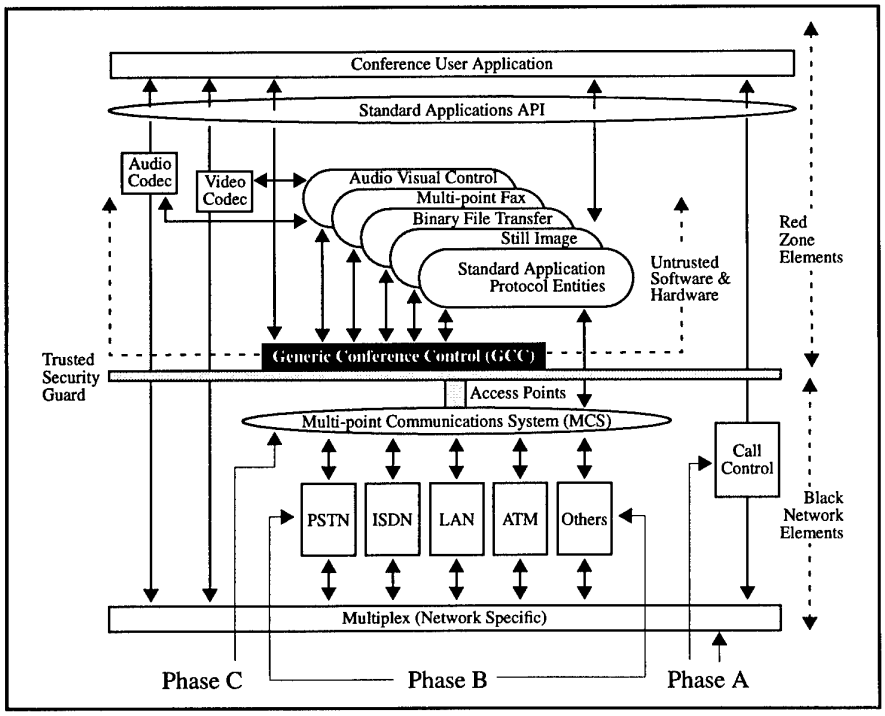

Figure 7 T.120 Conference Call Setup Procedures

The whole call setup is based on open untrusted communications. The main purpose of the call setup is to have the potential participants connected to the common network resources, namely the netted MCUs, in order to participate in a conference. In that sense, not many security functions can be supported. Particularly, conference-wide security is not possible because no individual end-points can be confident of the actual identities of the others at this stage. Only the security guard function, which prohibits unauthorised information leakage through the open established connections, can be enforced at the individual end-points. The associated guard-enabling mechanisms may or may not require cryptographic-based

technologies[14]. They are provided by the trusted guard components of the security peripheral devices.

6.1.1 Phase A: (Q.931 User-Network Signalling Protocols)

Based on the ISDN user-network signalling interface for basic call control (ITU-T Q.931), a conference terminal (or a MCU) makes the call control so as to establish an ISDN or an ATM connection for communicating with a MCU (or another conference terminal respectively)[15]. The SETUP message of the originating side must include at least information elements of bearer capability (BC), low layer capability (LLC), and high layer capability (HLC), all of which are needed to recognise the communication capability at the other end of the connection. The BC indicates the information transfer rate (64 Kbits/s, 128 Kbits/s, or other multiple values of 64 Kbits/s). The LC concerns the physical layer multiplexing mechanisms. Choices include ITU-T H.242[16] in the case of ISDN connection, and the system for utilising various ATM adaptation layer (AAL) types in the case of ATM connection. Finally, the HLC indicates that the calling side is capable of handling audio-only, audio-visual, audio-video, or multi-media[17].

Once the called side accepts a request to complete the connection and the physical connection is established, no further Q.931 signalling messages should be exchanged. The security peripheral device must block all further communications using the user-network signalling channel (Phase A in Figure 7). This prevents an attacker exposing the necessarily open channel connecting to the outside world. The blocking should be enforced regardless of whether the conference to be established will be classified or not.

6.1.2 Phase B: (H.242 or ATM Signalling Protocols)

After completing the connection over some physical media via Phase A, either the frame alignment conforming to ITU-T H.221 or the format enabling various AAL types should be used. Both can aggregate the throughput of one or more digital channels. In the case of an ISDN connection, which uses H.221, the total transfer rate is partitioned into static bit rate allocations for the individual media. However, the similar total transfer rate is shared dynamically by the interleaving ATM cells of the individual media in the case of an ATM connection. In either case, there are at least three types of virtual channels[18] carrying video, audio and T.120 data[19] (Figure 6).

---

14. Authorised readers may refer to one of the other associated projects of the TCS Group.
15. The recommendation in T.124 defines three main styles for a conference to be established: Meet-me, Call-out and Call-through. In the Meet-me style, all participants call into a MCU. In the Call-out style, the already connected MCUs set up the call by calling out to all participants. Finally, in the Call-through style, one participant calls into a MCU, then it adds other participants which are called by the MCU.
16. System for establishing communication between audio-visual terminals using digital channels up to 2 Mbits/s.
17. It would be appropriate to propose the inclusion of higher layer security capability indication into the standard.
18. The readers should not confuse virtual channels with the T.120-defined (group-oriented) logical channels discussed in Section 5.2. Virtual channels are defined in ISDN (including ATM) standards. They are multiplexed onto physical connections and so are effectively point-to-point only. On the other hand, group-oriented logical channels are multi-point by definition and may be accessed by multiple entities. They only exist at or above the MCS layer.
19. More channels or more types of channels are possible. Individual priority levels (Figure 8) can be assigned to these channels.

The security architecture must ensure that the video and audio virtual channel inputs are connected to the crypto engine outputs exclusively and to nowhere else (the audio and video codec blocks in Figure 7). This implies that the outgoing video and audio virtual channels are linked internally only to trusted components. A null encryption key may be used if the authorised human user wishes clear material[20] to be carried over some specific audio or video virtual channels. Finally, after each side recognises the other's capability, they decide their own communication mode including the common mode. That is, when both are sure of having the highest common T.120 capability, the MCS path is established, leading to Phase C.

6.1.3 Phase C: (MCS Protocols)

Before the MCS protocols are executed, the conventional peer-to-peer communications at OSI layers 2 to 4 or 2 to 7 (Figure 6) should be established over the point-to-point T.120 data virtual channels, which have been allocated within the physical ISDN or ATM connection in Phase B.

When the MCS protocols finally are negotiated, various static conference-wide MCS logical channels[21] are established automatically in order to recognise each other's conferencing functions and to enable information exchange by client applications like Generic Conference Control (GCC) or Still Image (SI). Within the security framework, some of the established MCS logical channels are used to initiate the negotiation of security relevant information for starting or establishing the necessary security functions required by military conferees. These functions include authentication, conversation information confidentiality and integrity, and secure multi-point still image or file transfer[22].

The aforementioned static MCS logical channels are vulnerable to attackers' exploitation via the open T.120 data virtual channels in the physical connection. It is not appropriate to protect these channels by encryption as they need to be accessed by open network elements, such as untrusted MCUs, in order to maintain a MCS domain. Nevertheless, unclassified security-relevant information should be exchanged readily over these "open" MCS logical channels when at least two participants are present (namely they are connected to a common MCU) for a conference to begin. As a result, except when activated by authorised trusted components, the security peripheral must prohibit the usage of these established MCS logical channels by guarding the MCS service access points (Figure 7), until the conference-wide security associations have been completed with all authorised conferees.

6.2 MCS User, Token, and Logical Channel IDs

The MCS layer provides 18 individual services to the client applications at its upper layers. These applications are called MCS Users in [30]. The associated MCS protocol data units (PDUs) are exchanged between peer MCS Providers in order to coordinate the services. These MCS services and associated PDUs are divided into 4 classes: Domain Management, Channel Management, Data Transfer, and Token Management.

The Domain Management allows a MCS Provider to become a part of a MCS domain hierarchy and to acquire a domain attachment membership for each of its client applications. The domain hierarchy typically consists of the MCS Providers at the MCUs and conference end-points. It is organised in the form of a tree where the root is the Top MCS Provider[23]. A

20. Obviously, this user instruction must be implemented in a trusted manner, and this may be provided via the trusted path between the human user and the security peripheral.
21. These channels are standardised, in terms of their Channel IDs, in T.122 and they may be used by various network entities, some of which may not be trusted.
22. More are listed in Section 6.3.

successful domain attachment[24] is indicated via the allocation of a User ID by the Top MCS Provider. Every User ID is treated as a single-member channel, which is allowed to be accessed by only the designated user. A user A who wishes to send information exclusively to another user B should send it over B's channel identified by B's User ID.

The Channel Management class is required when a client application wishes to convene, join, leave, disband, expand, and shrink a logical channel[25]. Associated MCS request PDUs are sent to the Top MCS Provider. In particular, the Top Provider confirms a channel convene request by issuing a Channel ID to the requester.

The Data Transfer class of services handles the transfer of information over some indicated logical channels upon receiving a request by an authorised client application. Finally, the Token Management class allows an application to grab, inhibit, give, request, release, and test a token[26], where the tokens simply provide a means to implement exclusive access to some specific resources.

6.2.1 Necessary Key Management Support

The important aspect of the MCS service coordination described in the above is that MCS services should not be trusted. For example, the User ID, dynamically issued by the untrusted Top MCS Provider, cannot be trusted for identifying a remote client application. Likewise, it should not trusted that the MCS would rigorously deny unauthorised access to some declared private channels.

However, it is the case that the MCS services should not be used at all to conduct conferences or group work. Instead, the user-control security capability should supplement those security critical MCS services. For example, if a channel should be private, the channel owner then must be able to activate the confidentiality function provided by the security peripherals so that he/she does not have to rely solely on the inherently untrusted MCS.

The following will discuss some of the MCS services, which require security supplements provided by the security peripherals, and the associated enabling key management support functions.

---

23. According to [27], the MCS Provider at the root of a MCS domain hierarchy is called the Top MCS Provider. It is the exclusive manager of all the Channel, User IDs and Token resources of the domain. The Top MCS Provider may or may not be located at a MCU. If it is, then the MCS domain hierarchy coincides with the MCU physical configuration of Figure 4.
24. One or more client applications of a MCS Provider can be attached to a MCS domain. Standard applications are Generic Conference Control, Audio Visual Control, Still Image. A non-standard application such as a security peripheral device also may be attached via a MCS access point and be assigned a conference-unique User ID.
Multiple copies of these applications are possible so that a copy of each is available to a single user to conduct his/her conferencing activities. Typically, a group of LAN users may share the resources of a MCS Provider belonging to their LAN. This MCS Provider may be connected to other MCS Providers over WANs as discussed in Section 6.1. Both standard applications and the security peripheral for a human user may be allocated at the user's terminal. Essentially, the LAN-based MCS Provider may be viewed as the local conferencing server for the local LAN-based users to communicate with remote users over WANs (Figure 9).
25. Only dynamic channels can be convened or disbanded. They also may be private depending on their ownership.
26. The allocation of a Token ID (and hence the corresponding token creation) is coordinated at the GCC layer [29]. Specifically, Token IDs are issuing by the Top GCC Provider. According to Section 7.1.2.1 of [29], the GCC Provider that receives the GCC-Conference-Create request primitive becomes the Top GCC Provider of the creating conference.

1. Proof and Non-repudiation of User ID Ownership and User ID Integrity:

   Before a client application can participate in a conference, it must obtain its associated User ID from the Top MCS Provider via the MCS-ATTACH-USER service. During the conference, the client application will be known as its associated User ID. Therefore, both User ID integrity and the ability to prove the ownership of a User ID are necessary security requirements. Hence, after receiving the User ID from the Top MCS Provider, the local security mechanism must apply the necessary cryptographic techniques to support the above two requirements via the associated digital signature. In addition, the User ID also must be protected from the "replay" attack by using time-stamping and/or a randomly generated nonce.

2. Proof and Non-repudiation of Channel Ownership and Channel ID Integrity:

   A client application acquires a channel with the associated Channel ID from the Top MCS Provider via the MCS-CHANNEL-CONVENE service. Similar to the case of User ID, after receiving the Channel ID, the local security mechanism must apply the necessary cryptographic techniques to provide the associated digital signature. In addition, the Channel ID also must be protected from the "replay" attack by using time-stamping and/or a randomly generated nonce.

3. Proof and Non-repudiation of Token Registration and Token ID Integrity:

   A client application may request a token from the Top GCC Provider via the GCC-REGISTRY-ASSIGN-TOKEN service, in order to coordinate a conference-wide application service with peer applications. This GCC service makes use of the MCS-SEND-DATA service to transport its GCC request PDU. The only way to identify the originator of the GCC request is to look for the User ID belonging the MCS-SEND-DATA PDU, which carries the GCC request PDU. A stronger GCC PDU authentication based on some cryptographic techniques would be essential because the unprotected MCS-SEND-DATA service PDUs can be vulnerable to malicious modification. The different ways to use the cryptographic techniques will depend on the trustworthiness of and adequate security protection for the Top GCC Provider[27], which issues the Token IDs.

4. Confidentiality and Integrity of Private Channel Data, and MCS-SEND-DATA and MCS-UNIFORM-SEND-DATA PDU user-data field:

   There are two typical mechanisms to transport conference conversation data (including text, audio, and video) and client application information among authorised conferees. The first is to deliver the (predominately audio or video-based) information directly into the conference-wide or sub-conference-wide dynamic private channels. These logical channels may be mapped directly onto the corresponding virtual channels in the physical connections and therefore skip both the MCS layer and OSI Layers 2 to 4 (or 2 to 7) (Figure 6 and Figure 8). The other mechanism is to make use of the MCS-SEND-DATA and MCS-UNIFORM-SEND-DATA services. Application information is encapsulated within the user data field of the respective PDUs, with an appropriate Channel ID indication. Through OSI Layers 2 to 4 (or 2 to 7), these PDUs then are carried by the T.120 data virtual channels in the physical connections (Figure 6 and Figure 8).
   Regardless of which mechanism is used, some conference conversation or application control information inevitably would require the confidentiality and integrity protection from external threats outside the conference. Additionally, the same protection also is

27. The trustworthiness of GCC Provider is discussed in Section 6.3.

required within the conference as a conferee may not wish to broadcast some of his information to the entire conference but only to a selective subset of authorised conferees. Such (internal and external) threats therefore call for the key management capability to establish multiple independent active session keys among multiple subsets as well as the whole set of authorised conferees.

6.3 Trustworthy Roles of GCC Provider and Top GCC Provider

This subsection will examine an important class of elements of the T.120-based multi-point communications platform. This class is called GCC Provider and it consists of two types: the ordinary type, whose elements are named simply GCC Provider, and the special type, whose elements are named Top GCC Provider. It is recognised that the functions of GCC Providers are primarily security-critical. Consequently, it prompts the investigation of a cost-effective method to assure the trustworthiness of the GCC Providers.

In Section 6.3.1 below, the GCC Providers' functions and their security relevancy are examined. The dependencies on valid conferees' identities then are emphasized in Section 6.3.2. Subsequently in Section 6.3.3, the incorporation of conference-wide security functions with security-critical GCC functions is proposed. Finally, Section 6.3.4 will discuss a possible security architecture for the T.120-based multi-point communications platform based on the security-reinforced GCC Providers.

6.3.1 T.120-based GCC Providers' Functions

The T.124 Recommendation [29] specifies the Generic Conference Control (GCC) functional component. This component encompasses such functions as conference establishment and termination, managing the roster of nodes participating in a conference, managing the roster of applications and application capabilities within a conference, registry services for use by the applications, coordination of conference conductorship, as well as other miscellaneous functions. These functions are executed by the agents known as GCC Providers, each of which is located at a user terminal or a MCU.

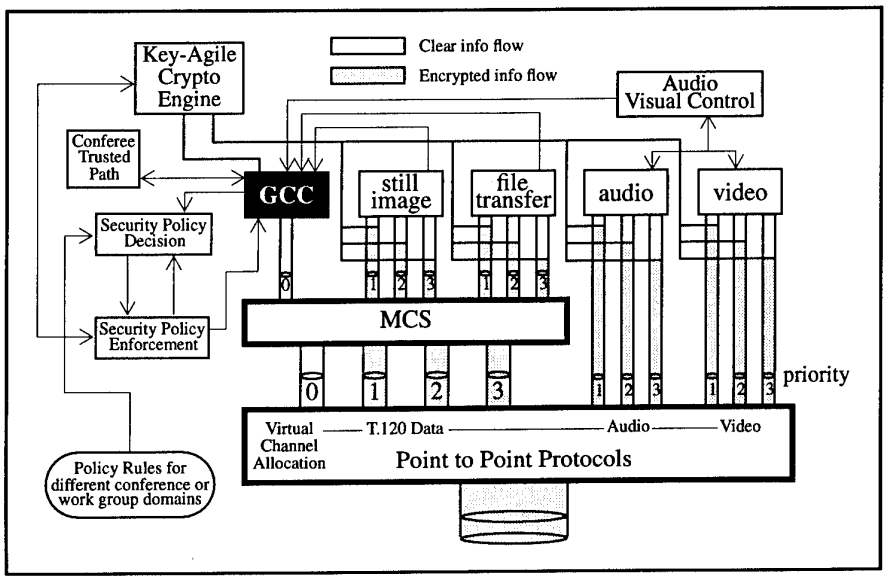

Figure 8 Interfaces between Security Mechanisms and T.120 Components

In terms of the T.120 protocol stack (Figure 8), every GCC Provider is an implementation of the GCC layer and it receives the MCS services from its local MCS Provider. It also interacts with other local client applications such as Audio Visual Control, Digital Fax Distribution, and Multi-point Still Image and Binary File Transfer in order to support their functions. Either individually or collectively, GCC Providers make use of the T.120-defined GCC functions to provide service supports for virtual conferences that closely mimic those of physical meetings.

It later shall seen that the GCC Provider at every classified user's terminal is protected by a unique local security peripheral device. After activated by the user, the security peripheral must obtain the necessary security relevant information about the user[28]. Various trusted components of the local security peripheral (Figure 8) are required to intercept the GCC Provider's actions for manual review and confirmation, and to interface with the GCC Provider in order to supplement its security-critical actions with appropriate cryptographic-based techniques.

6.3.1.1 GCC-Enabled Conference Service Supports

Examples of the conference service supports that are enabled by GCC Providers are outlined in the following list. While some of these can be obtained directly from the GCC Providers based on the individual standardised GCC primitives via the GCC service access points, others would require some combined activation of GCC primitives and possibly further assistance from other applications. This further assistance is expected in some areas to support certain functionality specified in [5]:

1. creating a conference;
2. creating and viewing a conference profile;
3. broadcasting conference and application rosters;
4. restricting access to a conference;
5. locking and unlocking a conference;
6. invitation to join a restricted conference;
7. designating authority by the conference convener;
8. assigning, request, transferring, or accepting the conductorship during a conference;
9. announcing the identity of the current conductor;
10. ejecting a particular conferee by the convener;
11. imposing orderly participant behaviour to the course of a conference by the conductor;
12. restricting a specific conferee to either hear, view, speak, send data, receive data, or any combinations of the above to all or some specific subset of conferees;
13. authorising special conference privileges to specific conferees;
14. merging multiple conferences;
15. splitting a conference into two or more;
16. forcibly terminating the entire conference at any time by the convener;
17. finding out what conferences are in progress;
18. joining or leaving a conference;
19. announcing a conferee's presence by the concerned conferee, the convener, or conductor;
20. identifying which client applications are available at each node;
21. collectively determining a common set of application capabilities;
22. enabling an authorised conferee to conduct private conversation or to distribute private information among selective conferees;
23. sponsoring or guaranteeing an individual for inclusion momentarily in the conference,

28. The procedures for the security peripheral to identify the user and to obtain the user's security relevant information are described in separate papers under another project of the TCS Group.

valid only while the sponsor or guarantor remains in the conference;
24. finding out how much time remains in a timed conference;
25. requesting more time to be added, if available;
26. manual termination by an explicit request;
27. automatic conference termination when all conference nodes are disconnected or when the conference time is up;
28. transmission of simple text messages;
29. requesting assistance from an operator.

6.3.2 Dependency on Valid Identity

There is one common characteristic among the above conference service supports. It is the dependency on the validity of conferees' identities, including that of the conference convener and current conductor. Without the certainty of valid identities of the initiators or objects, none of the above service supports can be effective. In fact, an entity should not be considered part of a conference until it has announced its presence with all the necessary authentication information given, via GCC-Conference-Join and GCC-Conference-Announce-Presence services.

Typically, the GCC-Conference-Join service is activated immediately after the completion of MCS-layer communications. At this point, the activator must have acquired the conference-wide User ID from the Top MCS Provider. On behalf of the activator, the local GCC Provider sends the GCC-Conference-Join request PDU (containing the activator's User ID) to the Top GCC Provider (usually controlled by the conference convener) to start the negotiation for the activator to join the conference. It therefore implies that a cryptographic-based mutual conferee authentication protocol should become a part of the negotiation. Additionally, the User ID, contained in the request PDU, should have been accompanied by the activator's digital signature in order to indicate its ownership. The signed User ID later can be distributed in the conference when the activator announces his/her presence. Enabling key management support with respect to User ID, Channel ID, and Token ID authenticity and integrity has been discussed in Section 6.2.1. The associated key management schemes can be incorporated into the appropriate GCC protocol exchange procedures. Descriptions of these schemes will be discussed in separate papers. A particular class of schemes based on multiple certification is described in [41].

6.3.3 Combining Conference-wide Security functions with GCC Functions

All communication and network security functions must begin with identity, mutual conferee, or object authentication. It therefore becomes natural that the conference-wide security functions (enabled by the security peripherals) are placed above the MCS layer[29] and are combined with the GCC functions (Figure 6 and Figure 7).

There also is another crucial rationale for the combinations. This is the skepticism about the GCC Provider's system ability to ensure integrity. One cannot guarantee that the GCC Provider always performs its functions to furnish the above conferee service supports and resists malicious attacks. It is therefore critical that the service supports be supplemented by the thorough execution of some cryptographic-based security protocols. These protocols are current being developed under another project of the TCS Group, IT Division of DSTO. Some of them are described in [42]. They include those for common sharing of a session channel key among authorised conferees and for enforcing subconferences. Others will be specified and mathematically verified in separate papers.

29. As argued in Section 6.2, the MCS layer is assumed to be untrusted.

6.3.4 Security Mechanisms for T.120-based Platform

According to Section 7.1.2.1 of T.124 recommendation [29], the GCC Provider that receives the GCC-Conference-Create request primitive becomes the Top GCC Provider of the conference being created. The Top GCC Provider has the responsibilities not required of other GCC Providers in a conference. The participant that issues the request primitive is called the conference convener and the terminal where the convener resides is called the convener node.

The recommendation requires that support for all forms[30] of this GCC-Conference-Create service is mandatory in every terminal. In other words, every user terminal should have the ability to become a convener node.

A security architecture for the T.120-based multi-point communications platform is illustrated in Figure 9. The architecture describes core elements within a sensitive LAN that need to be protected. A MCS Provider, which serves all users in the sensitive LAN, is allocated at the LAN gateway that is connected to the outside world via possibly public WANs. This is where connections to remote participants or open MCUs are set up, as discussed in Section 6.1. The LAN security guard mechanism is placed just in front of the MCS access points at the gateway. It allows only authorised information to get through to the access points. In this architecture, the GCC Providers at the end-point terminals, where the participants are present, need to be trusted. Moreover, there should exist a trusted path between each participant and his/her associated local GCC Provider.

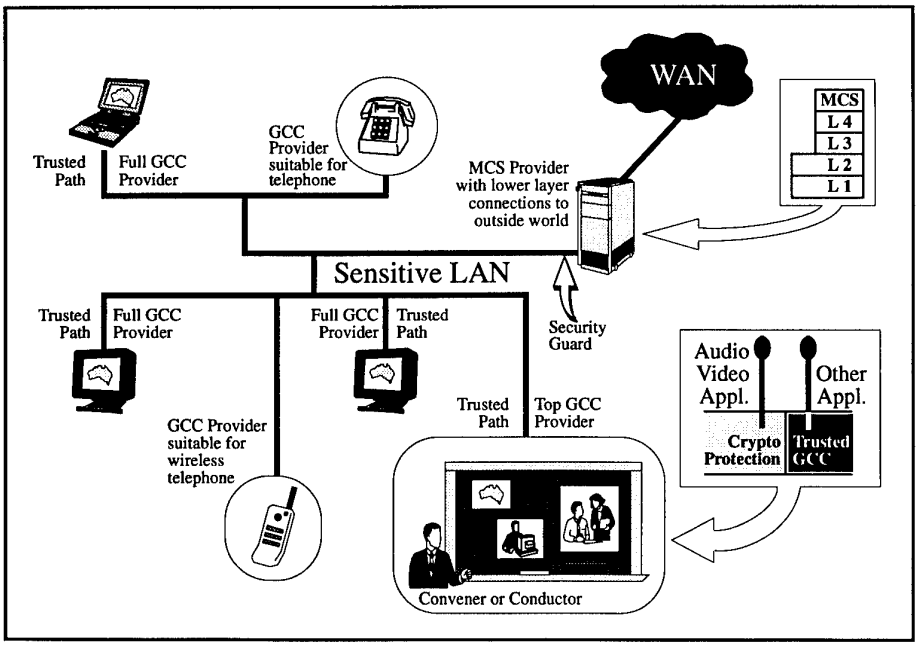

Figure 9 Security Architecture with Trusted GCC Providers in a Sensitive LAN

30. They are the usual request, indication, confirm, and response primitives.

6.3.4.1 Provision of Trusted GCC Providers and Associated Trusted Paths

Security-relevant actions of a GCC Provider can be reviewed and confirmed locally due to the participant's trusted path to the security peripheral. These actions concern mainly the submissions of various GCC service request and response PDUs. Information items are contained in the associated parameter fields, particularly the user data field. These information items must be reviewed manually in order to gain the necessary authorisation to get past the security guard mechanism and then through to the LAN gateway and beyond. With a valid authorisation, the participant then can confirm the submission of a reviewed GCC PDU. At a receiving end, the incoming GCC service indication and confirm PDUs also must be validated by the local security peripheral for their authenticity and integrity.

As a result, the participant controls his/her local GCC Provider's actions directly. It is the combination of

- MCS access point security guard; and
- manual revision and confirmation of GCC security relevant actions; and
- reinforcement of GCC security-critical functions by security functions based on a military-grade cryptographic key management scheme

that essentially transforms an ordinary GCC Provider into a trusted GCC Provider (Figure 8 and Figure 9).

6.3.4.2 Undesirability of Remote Top GCC Provider in Classified Conference

The convener of a conference is allowed by T.124 to issue the GCC-Conference-Create request remotely as well as locally. The security architecture however demands that, for classified conference creation, the convener only should issue the request locally. He/She therefore turns his/her (local) trusted GCC Provider into the trusted Top GCC Provider of his/her conference. There are at least two reasons to support this architectural demand.

1. The first reason is that it becomes necessary to consider the case where the Top provider is located remotely at a possibly untrusted MCU if the Top GCC provider may be activated remotely by the convener. The communications between the convener and the Top GCC Provider essentially are supported by the standardised GCC services. The PDUs of these services are encapsulated within some MCS service PDUs for transportation. Since the MCS layer is untrusted and there are no protection mechanisms for the MCS PDUs, additional security functions therefore must be made available to ensure a trusted path between the convener and the Top GCC Provider[31]. Moreover, the MCU, at which the Top GCC resides, may belong to the open network and is assumed to be untrusted. It is not effective to try to place a trusted element, namely the Top GCC Provider, into a potentially hostile environment, namely the open MCU, which may be exposed to malicious attacks. As a result, there exists the problem of securing a classified conference based on an untrusted Top GCC Provider.

2. With the association of the untrusted Top GCC Provider in a classified conference, the security protocol necessary for establishing the security association among the authorised conferees becomes more complicated. A trusted path between the convener and an untrusted Top GCC Provider is meaningless. When an authorised conferee receives some information or request for action from the Top GCC Provider, he would need to have an additional confirmation from the convener over another channel, which excludes the Top GCC Provider. Moreover, certain conference-specific information such as participant list could be too sensitive to be stored without protection in the con-

31. A trusted path exists between the convener and his/her local GCC Provider. It is the non-existence of a trusted path between the local GCC Provider and the remote Top GCC Provider that presents the problem.

ference application registry of the untrusted Top GCC Provider. This therefore requires additional cryptographic-based protection for the sensitive application registry information at the Top GCC Provider. Authorised participants also need to have secure mechanisms to retrieve and unravel the protected registry information. All these cryptographic supports would place far more overhead in the security protocol exchange procedures than is desirable or reasonable.

6.3.4.3 Security-Critical Activities of the Trusted Top GCC Provider

For the convener to have the Top GCC Provider (which is also his GCC Provider) locally rather than remotely, the trusted path between the convener and the Top GCC Provider would not need to be extended to a remote node. The trusted path between the convener and the Top GCC Provider is essentially that between the convener and his local GCC Provider. The Top GCC Provider's actions therefore would be under the conference convener's direct control and manual revision. Following the reasoning in Section 6.3.4.1, the Top GCC Provider at the convener's terminal also is trusted. This should mean that the conference-wide security association establishment protocol would become simpler and that the conference convener is provided with a stronger cryptographic-based control over his/her conference. Because of the trustworthiness of the Top GCC Provider with respect to the convener, the sensitive conference application registry information items, allocated at the Top GCC Provider, can be handled relatively easily. The only major security concerns for these information items are their confidentiality and integrity during transportation, over open networks, to authorised conferees. These however can be satisfied easily by encryption-based protection with a conference or sub-conference wide session channel key.

6.3.5 Where the T.124 Recommendation could be Improved

There are many places in the T.124 recommendation and generally the superset T.120 series of recommendations where security-related improvements can be made. Most notable is the transportation of passwords in the clear for creating and joining a locked conference (Sections 7.1.2.1 and 7.1.2.3 of T.124 [29] respectively). It may be appropriate for Defence to identify the security deficiencies and to use its influence in standards bodies to promote the correction. This ensures a shaping role for Defence in the setting of standards without the implication that Defence necessarily must provide resource to correct the deficiencies. The core Defence resources could be concentrated on Defence's own security architecture for supporting the T.120-based communication platform. Since Defence's security requirements in using the communication platform rely on its own security architectural protection and not on the security (such as password-based protection) inherently provided by the standardised platform, Defence therefore should influence the recommendations specifically in matters that could impact its own security architecture. In the following, two concerns in T.124 recommendations are presented. The corresponding recommendations could improve the functionality of the security architecture described in this section. Neither of these two proposed modifications should pose any huge overhead on the T.124 GCC protocol exchange procedures.

1. <u>De-coupling the Top GCC Provider from the Top MCS Provider:</u>

   The T.124 recommendation presents two definitions for the Top GCC Provider. According to Section 3.34 of [29], "*GCC Provider* (is): *the GCC Provider which is co-resident with the Top MCS Provider in a conference. ..... The location of the Top GCC Provider remains unchanged for the duration of a conference.*". In Section 7.1.2.1 of [29], "*the GCC-Conference-Create request primitive is used by a Node Controller* (which is a participant's interface at his/her terminal) *to create a new conference at a remote node* (which could be a MCU) *to which the local node is automatically*

joined. ..... When a conference is created, the node to which the creation request is directed (the node which receives the GCC-Conference-Create indication) is also automatically joined to the conference and becomes the Top GCC Provider for that conference. In some implementations, it may be possible to create a conference locally without the use of GCC primitives. In this case, the node at which the conference is created becomes the Top Provider."

It has been argued in Sections 6.3.4.2 and 6.3.4.3 that, at least for classified conferences, the convener should issue the GCC-Conference-Create request locally and turn its local GCC Provider into the Top GCC Provider, based on the security architectural protection. It therefore follows from the above definitions that the convener must reside at a MCU because (1) the Top GCC Provider is located at the convener; (2) the Top GCC and MCS Providers are co-located at the same node; and (3) the Top MCS Provider typically resides at a MCU. In theory, it is not a concern that every participant who wishes to create a conference must have access to a MCU. In practice, this becomes a problem because of the relatively high cost of the MCUs. After examining the draft T.124 recommendation [29], it is considered that the Top GCC Provider technically need not be required to co-reside with the Top MCS Provider. None of the standardised functionality of T.124 is altered if the Top GCC and MCS Providers are located at separate nodes. Therefore it is recommended that the approval from ITU-T SG 8 should be sought for removing the unnecessary restriction of the co-residence of Top GCC and MCS Providers.

2. Dynamically Transferring the Top GCC Provider's Role from the Current Authorised Conference Conductor's Local GCC Provider to that of the Next Conductor:

The T.124-definition of the Top GCC Provider states that once a GCC Provider becomes the Top GCC Provider, it retains its role as long as the conference continues to exist. The convener of a conference is allowed by T.124 to leave and rejoin the conference from time to time. During his/her absence, he can authorise a specific conferee to become the conference conductor who would receive special privileges granted by the convener. However, according to T.124, the Top GCC Provider's role is not transferred to the conductor's local GCC Provider. This means that the Top GCC Provider is left on its own to look after the (sometimes security-relevant) conference-wide information data bases such as application registry, conference profile, and conference and conference application rosters. Since the trustworthiness of GCC Provider cannot be established completely without a participant's presence (Section 6.3.4.1), there exists the problem of secure conference-wide information data base handling by the Top GCC Provider that becomes untrusted during the convener's absence.

As a result, it is recommended that the Top GCC Provider's role should be made transferable. Specifically, a mechanism should be provided in the GCC layer to transfer the Top GCC Provider's role to the local GCC Provider of the appointed conference conductor. That is, the conference-wide information data bases can be moved securely from the convener's node to the conductor's node. Similarly, when the conductorship is transferred from the current to the next conductor, the role of the Top GCC Provider should be moved also to the next conductor's local GCC Provider. Finally, when the convener rejoins the conference, the role of the Top GCC Provider also would be returned to his/her local GCC Provider.

6.4 Further Work

More work is required to address the appropriate security supports for other group-oriented services, including Multi-point Digital Fax Distribution, and Still Image and Binary File Transfer, and others. Continuous monitoring of the standardisation of the T.120 protocols is necessary.

As far as the core security architectural components for a T.120-based multi-point communications platform are concerned, ongoing research is being conducted by the TCS Group. These efforts include a military-grade key management scheme, various security protocol supports, trusted security guard mechanisms, implementation of trusted paths, and others. Additionally, this paper assumes the presence of and hence implies the need for a key agile cryptographic engine, which allows multiple streams of information data to be encrypted with independent distinct keys. Currently, key agile encryption is being focused on ATM cell streams [43]. However, it has been shown in this paper that ATM cell encryption is superfluous within the security architecture for a T.120-based real-time multi-media multi-point communication platform. Key agile encryption is nevertheless effective when it is applied at places close to the data stream sources.

This is a blank page.

7 Conclusion

This paper has identified a set of internationally-standardised protocols which can be used to support real-time, multi-media, multi-point communication platforms. The relevant standards are called the T.120 series of recommendations developed by the International Telecommunication Union. The major benefit of this technology is its potential for introducing the 'BLACK conferencing' capability, where dedicated conference bridges or multi-point control units are not required to process RED conference information.

The paper specifically focuses on the trustworthiness of a group-oriented communication platform-enabling mechanism called GCC (Generic Conference Control) Provider because of its security-relevant actions and conference service supports. To allow greater flexibility with respect to the security architecture support, two concerns have been identified in the T.124 recommendation of GCC Specification where Defence may exercise its influence.

This is a blank page.

8 Reference

[1] 'Strategic Review 1993'. DPUBS: 8009/93. Defence Centre - Canberra. Nov. 1993.

[2] Billard B. and Anderson M. 'The Military Infosec Dilemma and a Possible Australian Response'. Defence Science and Technology Organisation. DSTO-TR-0123. Dec. 1994.

[3] 'Defending Australia' Defence White Paper 1994. Australian Government Publishing Service. Canberra. Dec. 1994.

[4] 'Defence Annual Report 1993-1994'. Australian Government Publishing Service. Canberra. Oct. 1994.

[5] Anderson M., Fiddyment C., Klink M., Lai M.K.F., Parker N., Shoubridge P., Sutherland M., Yesberg J. and Yiu K. 'D6 Security Architecture Illustration Version 1.5'. DSTO-GD-0030. Defence Science and Technology Organisation. Sep. 1994.

[6] Andrews B. 'The DORIC Program'. Defence Science and Technology Organisation. DSTO-paper. Dec. 1994.

[7] 'A Security Architecture for Large, Distributed Multimedia Systems'. Defence Science and Technology Organisation Task Plan ADF93/256. N8316/8/17. Feb. 1994.

[8] 'Defense Information System Network (DISN) Architecture'. Baseline coordination draft, Defense Information Systems Agency, DISN-AR-1000, 1993.

[9] DDNS Minute DGFD(J) 1252/94 dated 12 Sep. 94.

[10] DIS-N Minute DIS-N 316.94 dated 27 Oct. 94.

[11] Chadderdon R.A. 'United States Special Operations Command (USSOCOM) Phase 1 Video Teleconferencing (VTC) Architecture'. 1994 IEEE MILCOM Conference Record, Oct. 2-5, 1994, Ft. Monmouth. pp. 92-96. 1994.

[12] Deville J. and King C.A. 'Interoperability Issues of Existing Collateral Video Teleconferencing Systems at the United States Pacific Command'. 1994 IEEE MILCOM Conference Record, Oct. 2-5, 1994, Ft. Monmouth. pp. 97-101. 1994.

[13] Mooney F.W., Newport K.T. and Schroeder M.A. 'Video Teleconferencing (VTC) in an Integrated Digital Network Exchange (IDNX)-Based Communications System'. 1994 IEEE MILCOM Conference Record, Oct. 2-5, 1994, Ft. Monmouth. pp. 102-106. 1994.

[14] Brundage J.H. 'Use of Video-Teleconferencing in Tactical Operations'. 1994 IEEE MILCOM Conference Record, Oct. 2-5, 1994, Ft. Monmouth. pp. 107-111. 1994.

[15] Gilder G. 'The Bandwidth Tidal Wave'. Forbes ASAP. 5 Dec. 1994.

[16] Anderson M., Hayman K., Marriott D., Yesberg J., Nayda L. and Beahan B. 'P1 Prototype Stubs: an Overview'. ERL-0668-RR. Defence Science and Technology Organisation. Nov. 1992.

[17] DGFD (Joint) Minute DGFD (J) 1262/94 dated 27 Oct. 94.

[18] Thom G.A. 'Characteristics of Tactical Video Systems'. 1994 IEEE MILCOM Conference Record, Oct. 2-5, 1994, Ft. Monmouth. pp. 232-236. 1994.

[19] Fitzpatrick S.K. and Hargaden P.J. 'Multimedia Communications in a Tactical Environment". 1994 IEEE MILCOM Conference Record, Oct. 2-5, 1994, Ft. Monmouth.

pp. 242-246. 1994.

[20] Zieniewicz M.J. and Flatt J.D. 'An Overview of Video Compression Techniques and Applications for The Soldier's Computer/Radio'. 1994 IEEE MILCOM Conference Record, Oct. 2-5, 1994, Ft. Monmouth. pp. 252-256. 1994.

[21] Leeds M. 'Desktop Videoconferencing'. MACWORLD. pp. 87-92. Nov. 1994.

[22] Heinrichs B. and Jakobs K. 'An Enhanced Communication Architecture to Support Multi-media Group Communication'. Proceedings of Local and Metropolitan Area Networks, Apr. 5-6, 1993, Berlin. pp. 56-67. 1993.

[23] Szuprowicz B.O. 'Multimedia Networking and Communications'. 1st Edition. Computer Technology Research Corp. 1994.

[24] Ishii H., Kobayashi M. and Arita K. 'Iterative Design of Seamless Collaboration Media'. Communications of the ACM. Vol. 37, No. 8, pp. 83-97. Aug. 1994.

[25] ITU-T Recommendation H.200 'Framework for Recommendations for Audiovisual Services'. Mar. 1993.

[26] ITU-T Recommendation T.120 'Transmission Protocols for Multimedia Data'. Draft. Nov. 1994.

[27] ITU-T Recommendation T.122 'Multipoint Communication Service for Audiographic and Audiovisual Conferencing'. Draft. Jul. 1994.

[28] ITU-T Recommendation T.123 'Protocol Stack for Audiographic and Audiovisual Teleconference Applications'. Draft. 1994.

[29] ITU-T Recommendation T.124 (also known as T.GCC) 'Generic Conference Control for Audiovisual and Audiographic Terminals and Multipoint Control Units'. Draft. Apr. 1994.

[30] ITU-T Recommendation T.125 'Multipoint Communication Service Protocol Specification'. Draft. 1994.

[31] ITU-T Recommendation T.AVC 'Audio Visual Control Protocol Specification'. Draft. Nov. 1994.

[32] ITU-T Recommendation T.126 'Multipoint Still Image and Annotation Protocol'. Draft. Oct. 1994.

[33] ITU-T Recommendation T.127 'Multipoint Binary File Transfer Protocol Specification'. 1994.

[34] 'Chattering Heads Finds Common Tongue'. The Australian. 8 Nov. 1994.

[35] Semilof M. 'IBM Takes on Intel in Video'. CommunicationsWeek International. 24 Oct. 1994.

[36] Semilof M. 'Desktop Conferencing Conflict Erupts'. CommunicationsWeek International. 28 Nov. 1994.

[37] 'Multi-point Multi-media Conferencing Unit, Issue 2'. Generic Requirements GR-1337-CORE. Bellcore Bell Communications Research. Sep. 1994.

[38] 'Microsoft and DataBeam Announce Data-Conferencing Technology Relationship: Mircosoft Licenses DataBeam's T.120-Based Tools To Build Real-Time, Multi-point Applications'. Mircosoft Corp., Redmond, Wash., and DataBeam Corp., Lexington, Ky. Feb. 1995.

[39] 'Telstra Multi-media Conferencing Trial Program'. Formal Communication with Telstra Enhanced Services, Multi-Media Conferencing Group, Telstra Corp. Ltd., Feb. 1994.

[40] 'Speakeasy Applications Cookbook'. Telecom Australia (a trading name of Telstra in Australia), 1992.

[41] Lai M.K.F. and Anderson M. 'Schemes for Multiple Certification and Mailing List Ordering'. Draft DSTO Report. Oct. 1994.

[42] Lai M.K.F. 'A Configuration for BLACK Audio Conferencing Using ISDN Phones'. Draft DSTO Report. Oct. 1994.

[43] Semancik W.J., Mercer L.B., Hoehn T.W., Rowe G.D., Smith-Luther M.P., Agee R.C., Fowlkes D. and Ingle J.T. 'Cell Level Encryption for ATM Networks and Some Results from Initial Testing'. Department of Defense, Ft. George G. Meade, MD 20755-6000. 1994.

This is a blank page.

Secure Real Time Group-Oriented Communications

Distribution

DEPARTMENT OF DEFENCE

Science and Technology

Defence Science and Technology Organisation Central

Chief Defence Scientist and members of the	)
DSTO Central Office Executive	) 1 shared copy
Counsellor, Defence Science, London	Cont Sht
Counsellor, Defence Science, Washington	Cont Sht
Senior Defence Scientific Adviser	1 copy
Scientific Adviser POLCOM	1 copy

Aeronautical & Maritime Research Laboratory

Director Aeronautical & Maritime Research Laboratory	1 copy

Electronics & Surveillance Research Laboratory

Chief Information Technology Division	1 copy
Chief Electronic Warfare Division	Cont Sht
Chief Guided Weapons Division	Cont Sht
Chief Communications Division	Cont Sht
Chief Land, Space and Optoelectronics Division	Cont Sht
Chief High Frequency Radar Division	Cont Sht
Chief Microwave Radar Division	Cont Sht
Research Leader Command & Control and Intelligence Systems	1 copy
Research Leader Military Computing Systems	1 copy
Research Leader Command, Control and Communications	1 copy
Manager Human Computer Interaction Laboratory	Cont Sht
Executive Officer (ITD)	Cont Sht
Head Software Engineering Group	Cont Sht
Head Trusted Computer Systems Group	1 copy
Head Command Support Systems Group	1 copy
Head Intelligence Systems Group	Cont Sht
Head Systems Simulation and Assessment Group	Cont Sht
Head Exercise Analysis Group	Cont Sht
Head C3I Systems Engineering Group	Cont Sht
Head Computer Systems Architecture Group	Cont Sht
Head Information Management Group	Cont Sht
Head Information Acquisition & Processing Group	Cont Sht
Author (M.K.F. Lai)	5 copies

Navy

Navy Scientific Adviser	1 copy

Army

Scientific Adviser, Army	1 copy

Air Force

Air Force Scientific Adviser	1 copy

Forces Executive

Director General Force Development (Joint)	1 copy
Director General Force Development (Land)	1 copy
Director General Force Development (Air)	1 copy
Director General Force Development (Sea)	1 copy
Director General Joint Communications and Electronics	1 copy
Deputy Director Network Systems	1 copy
Deputy Director Communications Engineering Support	1 copy

Acquisition and Logistics

Director General Information Management and Communications Engineering	1 copy
Director General Joint Projects Management	1 copy
Director Joint Communication Projects (Switching)	1 copy

Strategy and Intelligence

Assistant Secretary Scientific Analysis	1 copy
Assistant Secretary Information Security	1 copy

LIBRARIES AND INFORMATION SERVICES

Australian Government Publishing Service	1 copy
Defence Central Library, Technical Reports Centre	1 copy
Manager, Document Exchange Centre, (for retention)	1 copy
Defense Technical Information Service, United States	2 copies
Defence Research Information Centre, United Kingdom	2 copies
Director Scientific Information Services, Canada	1 copy
Library, Ministry of Defence, New Zealand	1 copy
National Library of Australia	1 copy
Defence Science and Technology Organisation Salisbury, Research Library	2 copies
Library Defence Signals Directorate Canberra	1 copy
British Library Document Supply Centre	1 copy
Parliamentary Library of South Australia	1 copy

The State Library of South Australia 1 copy

SPARES

Defence Science and Technology Organisation Salisbury,
Research Library 6 copies

This is a blank page.

Department of Defence

DOCUMENT CONTROL DATA SHEET

1. Page Classification	
UNCLASSIFIED	
2. Privacy Marking/Caveat (of document)	
NA	

3a. AR Number	3b. Laboratory Number	3c. Type of Report	4. Task Number	
AR-009-398	DSTO-RR-0055	RESEARCH REPORT	ADF93/256	
5. Document Date	6. Cost Code	7. Security Classification	8. No of Pages	52
SEPTEMBER 1995	840708	* U U U	9. No of Refs	43

10. Title

SECURE REAL TIME GROUP-ORIENTED COMMUNICATIONS

Document Title Abstract

S (Secret) C (Confi) R (Rest) U (Unclass)

* For UNCLASSIFIED docs with a secondary distribution LIMITATION, use (L) in document box.

11. Author(s)
M.K.F. Lai

12. Downgrading/Delimiting Instructions
NA

13a. Corporate Author and Address

Electronics & Surveillance Research Laboratory
PO Box 1500, Salisbury SA 5108

13b. Task Sponsor
HQADF

14. Officer/Position responsible for

Security: NA
Downgrading: NA
Approval for Release: CITD

15. Secondary Release Statement of this Document

APPROVED FOR PUBLIC RELEASE

16a. Deliberate Announcement

NO LIMITATION

16b. Casual Announcement (for citation in other documents)

[√] No Limitation [ ] Ref. by Author, Doc No. and date only

17. DEFTEST Descriptors
Secure Communications
Communications Networks

18. DISCAT Subject Codes
NA

19. Abstract

This paper is part of the document series produced under the HQADF sponsored task 'D6: A Security Architecture for Large, Distributed Multimedia Systems'. The first of two main aims of this paper is to identify an internationally standardised real-time multi-media multi-point communications platform, on which mission-centric group-oriented applications may be developed using commercially available products. The second aim is to investigate the protocol security requirements to support the identified platform. This paper specifically focuses on the trustworthiness of a platform-enabling mechanism known as GCC (Generic Conference Control) Provider. A potential outcome could imply the possibility of "BLACK Conferencing", where only encrypted conference information is processed by conference bridges or multi-point control units.